Sistema de Interceptação "ECHELON"
Sistema global de interceptação de comunicações privadas e econômicas

Alexandre Hosang
CAEPE
ESG

1 Introdução

Em 5 de junho de 2000, o Parlamento Europeu decidiu constituir uma comissão temporária para investigar o sistema Echelon que é uma tecnologia de ponta com processamento automatizado para fins de espionagem de sistemas de comunicações.

A decisão teve como base o relatório dedicado ao tema "Avaliação das técnicas de controle político", que o STOA[1] encomendara em nome do Parlamento Europeu em 1997 à Fundação Omega, no qual é feita uma descrição do sistema ECHELON no capítulo intitulado" Redes nacionais e internacionais de intercepção das comunicações". O autor do estudo afirma que todas as comunicações electrônicas, telefônicas e por fax, na Europa são quotidianamente interceptadas pela NSA[2]. Este relatório chamou a atenção de toda a Europa para a existência do sistema ECHELON, considerado um sistema de intercepção polivalente à escala mundial.

Uma afirmação contida num dos relatórios do STOA de 1999, de autoria de Duncan Campbell, constante no Relatório do Parlamento Europeu (2001), acabaria por suscitar grande polêmica:

> *"o Echelon já não prosseguiria o seu objectivo inicial de defesa face ao Leste, tendo passado a constituir um instrumento de espionagem económica. Este tese é fundamentada no relatório por exemplos de alegada espionagem económica, que teriam prejudicado em particular a Airbus e a Thomson CFS. Campbell reporta-se para o efeito a relatos da imprensa americana."*

2 Considerações Gerais

2.1 SIGINT

De acordo com o Manual estadunidense de Inteligência FM 2-0, INTELLIGENCE (2010), as disciplinas de inteligência são categorias de funções de inteligência, quais sejam:

> *Human Intelligence (HUMINT), Geospatial Intelligence (GEOINT), Imagery Intelligence (IMINT), Signals Intelligence (SIGINT), Measurement and Signatures*

[1] *Scientific Techonology Options Assessment* (Avaliação das Opções Científicas e Técnicas) - é um serviço da Direção-Geral de Estudos do Parlamento Europeu.

[2] *National Security Agency* (Agência de Segurança Nacional Norte-Americana).

Intelligence (MASINT), Open-Source Intelligence (OSINT), Technical Intelligence (TECHINT), and Counterintelligence (CI).

Dessas destaca-se a SIGINT que, segundo o referido manual, é a categoria da inteligência que compreende, individualmente ou de forma combinada, toda a inteligência de comunicações (Communications Intelligence – COMINT), Inteligência Eletrônica (Electronic Intelligence - ELINT) e Inteligência de Sinais de Instrumentos Estrangeiros (Foreign Instrumentation Signals intelligence - FISINT), transmitida de qualquer modo. Portanto, SIGINT é derivada das comunicações, da eletrônica e dos sinais de instrumentos estrangeiros.

Entende-se:

- COMINT como sendo a inteligência derivada de sinais eltromagnéticos de comunicações estrangeiros.

- ELINT como sendo a inteligência técnica e de georreferenciamento derivada sinais eltromagnéticos de não-comunicações estrangeiros, diferentes de detonações nucleares e atividades radioativas.

- FISINT como sendo informações técnicas e de inteligência derivadas de interceptação de emissões eletromagnéticas estrangeiras, associadas a distribuição operacional do espaço aéreo, da superfície, e dos sistemas subsuperficiais não estadunidenses.

O Relatório do Parlameto Europeu (2001) destaca que a exploração dos sinais eletromagnéticos de todo o tipo são interceptados, analisados e avaliados.

Ainda segundo o mesmo Relatório, o funcionamento desse tipo de sistema compreende que os sinais são captados por centrais fixas, satélites de órbita baixa ou satélites SIGINT geostacionários. Destaca-se, neste contexto, o seguinte aspecto:

> “os serviços de inteligência externa de muitos países interceptam as comunicações militares e diplomáticas de outros países. Muitos destes serviços vigiam igualmente, desde que a elas tenham acesso, as comunicações civis de outros países.”[3]

A tabela 1 dá uma panorâmica da situação que permite avaliar a atividade de interceptação dos serviços de inteligência, visando adotar um critério de comparação. Dele se deduz que a intercepção das comunicações privadas pelos serviços de informações externas não é uma particularidade dos serviços de informações norte-americanos ou britânicos.

---

[3] Parlamento Europeu, Relatório sobre a existência de um sistema global de interceptação de comunicações privadas e econômicas (sistema de interceptação “ECHELON”), elaborado por Comissão Temporária sobre o Sistema de Interceptação ECHELON, Portugal: 2001.

Tabela 1

Atividades de intercepção dos serviços de informações

País	Comunicações Exteriores	Comunicações públicas	Comunicações privadas
Bélgica	+	+	-
Dinamarca	+	+	+
Finlândia	+	+	+
França	+	+	+
Alemanha	+	+	+
Grécia	+	+	-
Irlanda	-	-	-
Itália	+	+	+
Luxemburgo	-	-	-
Países Baixos	+	+	+
Áustria	+	+	-
Portugal	+	+	-
Suécia	+	+	+
Espanha	+	+	+
Reino Unido	+	+	+
EUA	+	+	+
Canadá	+	+	+
Austrália	+	+	+
Nova Zelândia	+	+	+

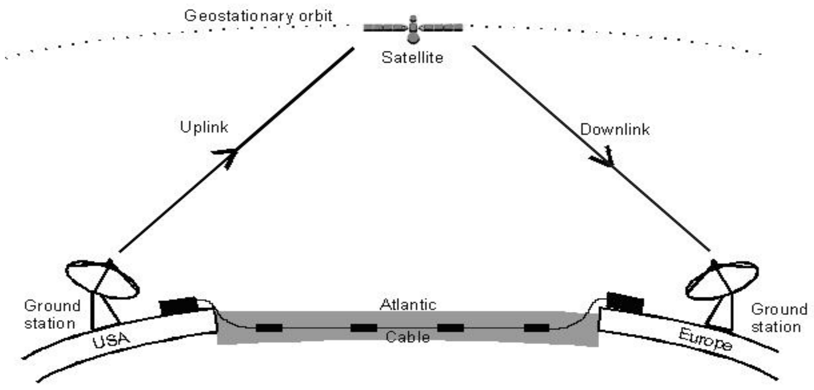
Fonte: Parlamento Europeu, 2001

2.2 Comunicações via satélite

É crescente a importância dos satélites de comunicações, pois os mesmos constituem hoje um elemento indispensável da rede mundial de telecomunicações e da difusão de programas de televisão e de rádio, assim como dos serviços multimídia.

A transmissão de sinais por satélites processa-se do seguinte modo: o sinal proveniente de uma linha é enviado para o satélite por uma estação terrestre equipada com uma antena parabólica através de um feixe de ondas eletromagnéticas ascendente, o denominado "uplink". O satélite recebe o sinal, reforça-o e o envia através de um feixe de ondas eletromagnéticas descendente, o denominado "downlink", para outra estação terrestre. Aí, o sinal é reencaminhado para uma rede de cabo. No caso das comunicações móveis (telemóveis que funcionam via satélite), o sinal é transmitido diretamente da unidade móvel de comunicações para o satélite, podendo ser daí novamente introduzido numa linha através de uma estação terrestre ou ser diretamente retransmitido para outra unidade móvel. Esquematicamente, o funcionamento é apresentado na figura 1.

Figura 1 - Esquema de ligação das comunicações via satélite



Fonte: Parlamento Europeu, 2001

Pode-se citar alguns exemplos de emprego de satélites de comunicações:

- comunicações telefônicas e de dados nacionais, regionais e internacionais em regiões com um reduzido volume de comunicações;

- comunicações no caso de intervenções em situações de catástrofe, manifestações e obras de construção de grandes dimensões;

- missões da ONU em regiões que não dispõem de infraestruturas de comunicações suficientemente desenvolvidas; e

- comunicação econômica flexível/móvel com microestações terrestres (V-SAT)

Os Satélites geoestacionários são colocados numa órbita circular paralelamente ao Equador e giram seguindo exatamente a rotação da Terra. Visto da superfície terrestre, o satélite encontra-se imóvel a uma altitude de cerca de 36000 km. A maior parte dos satélites de telecomunicações e de radiodifusão pertencem a este tipo de satélites.

Dentre as vantagens na utilização de satélites nas comunicações, destacam-se as seguintes:

- o raio de ação de um único satélite geoestacionário pode cobrir quase 50% da superfície terrestre, incluindo terrenos inacessíveis; e

- os satélites podem se tornar operacionais em poucos meses, independentemente da infra-estrutura local, e podem ser facilmente desativados

3 Echelon

3.1 Acordo UKUSA

O Acordo UKUSA constituiu a continuação da estreita cooperação já existente durante a Segunda Guerra Mundial entre os Estados Unidos e a Grã-

Bretanha, Canada, Australia e Nova Zelândia.

A intervenção dos Estados Unidos na Guerra contribuiu para um novo reforço da cooperação SIGINT. Em 1942, os criptoanalistas norte-americanos da "Naval SIGINT Agency" começaram a operar na Grã-Bretanha. A comunicação entre as salas de controle dos submarinos em Londres, Washington, e, a partir de maio de 1943, em Otava, no Canadá, tornou-se tão estreita que trabalhavam, como uma única organização.

Na primavera de 1943, foi assinado o acordo BRUSA-SIGINT, tendo igualmente tido lugar um intercâmbio pessoal. O conteúdo do acordo pode ser resumido nas suas três primeiras frases: intercâmbio de todas e quaisquer informações relacionadas com a descoberta, identificação e escuta de sinais, bem como decifragem e encriptação.

No pós-guerra, a iniciativa de manutenção de uma aliança SIGINT partiu essencialmente da Grã-Bretanha. Um dos objetivos visados consistia em enviar pessoal SIGINT da Europa rumo ao Pacífico, para a guerra com o Japão. Neste contexto, foi acordado com a Austrália a disponibilização de recursos e pessoal (britânicos) aos serviços australianos.

Em Setembro de 1945, Truman assinava um memorando altamente confidencial, que constitui a pedra angular de uma aliança SIGINT em tempos de paz. Seguidamente, foram realizadas negociações entre os Britânicos e os Americanos sobre a conclusão do acordo. Uma delegação britânica entrou em contato com Canadenses e Australianos, no intuito de debater uma eventual participação.

Em Fevereiro e Março de 1946, realizou-se uma conferência SIGINT anglo-americana, altamente confidencial, tendente a discutir os pormenores do acordo. Os Britânicos tinham recebido autorização dos Canadenses e Australianos. O resultado da conferência foi dado por um acordo secreto de cerca de 25 páginas, que selavam os pormenores de um acordo SIGINT, entre os Estados Unidos e a Commonwealth britânica. Nos dois anos subsequentes tiveram lugar outras negociações, tendo o texto definitivo, denominado Acordo UKUSA, sido assinado em Junho de 1948.

O Relatório do Parlamento Europeu (2001) apresentou que, durante um longo período de tempo, não existiu qualquer reconhecimento oficial do acordo UKUSA por parte dos Estados signatários. Porém. no relatório anual do “Intelligence and Security Committee” inglês, órgão de controle parlamentar do Reino Unido, o acordo UKUSA é expressamente mencionado:

> “A qualidade da informação recolhida reflete claramente o valor assumido pela estreita cooperação ao abrigo do acordo UKUSA. Esta tornou-se recentemente patente, quando o equipamento norte-americano da “*National Security Agency*” (NSA) colapsou e, durante três dias, quer a clientela norte-americana, quer a clientela britânica normal do GCHQ foram diretamente servidas por este último.”[4]

Portanto, o Acordo UKUSA previa a existência de uma cooperação de SIGINT, entre os Estados Unidos e a Commonwealth britânica, que a partir deste ponto será designado como “Echelon”.

O sistema Echelon distingue-se dos outros sistemas de informação pelo fato de apresentar duas características principais.

A primeira característica é a capacidade praticamente global de vigilância, recorrendo principalmente a estações receptoras via satélite e a satélites de espionagem, com a possibilidade de interceptar qualquer comunicação via telefone, telefax, Internet ou e-mail.

A segunda característica é o fato do sistema funcionar a nível mundial graças a uma cooperação entre vários países (Reino Unido, EUA, Canadá, Austrália e Nova Zelândia). Dadas as suas dimensões, é evidente que não é possível instalar estações receptoras de comunicações via satélite no território de um país sem o respectivo consentimento. Para tal, é indispensável o acordo mútuo entre vários países distribuídos pelo Globo. Os diferentes países que participam no sistema Echelon (Estados UKUSA) podem disponibilizar reciprocamente os respectivos dispositivos de escutas, partilhar entre si os encargos e utilizar em comum os resultados obtidos.

3.2 Estações de Interceptação

As estações de interceptação de Comunicações via satélite são divididas em dois tipos: as que apresentam indícios de sua finalidade e as outras que, de acordo com os critérios adotados pelo Parlamento Europeu, não permitem provar claramente a sua missão.

Do Relatório do Parlamento Europeu (2001), destacam-se as seguintes conclusões:

- em cada área abrangida pelos "global-beams"[5], das principais redes de satélites de comunicações civis, existe pelo menos uma antena do sistema de interceptação satelital. As estações são operadas por americanos ou ingleses, que exercem aí atividades de serviços de informação;

---

[4] Parlamento Europeu, Relatório sobre a existência de um sistema global de interceptação de comunicações privadas e econômicas (sistema de interceptação “ECHELON”), elaborado por Comissão Temporária sobre o Sistema de Interceptação ECHELON, Portugal: 2001

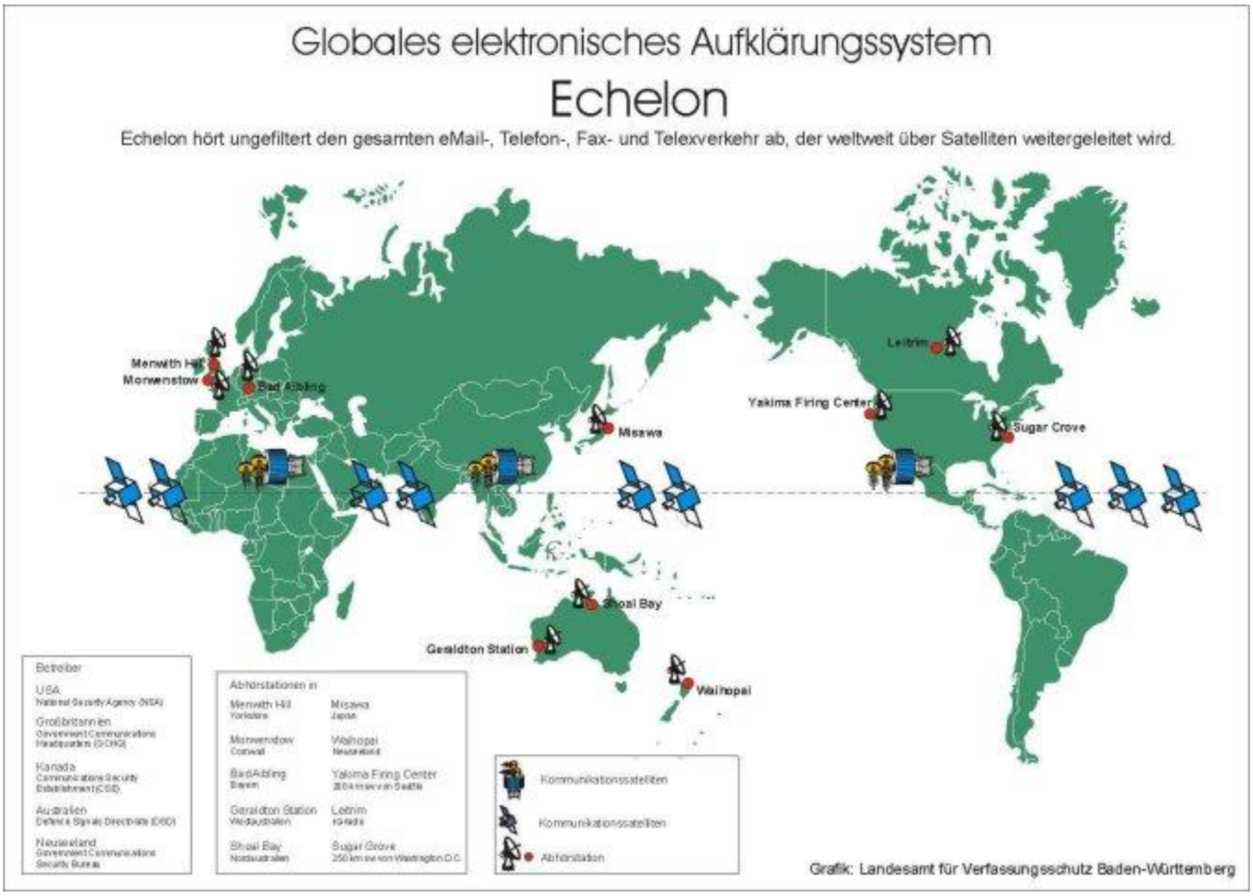
[5] Área do globo terrestre abrangida por um satélite.

- o desenvolvimento da comunicação INTELSAT[6] e a criação simultânea das respectivas estações de intercepção são uma prova da orientação global do sistema; e

- algumas das estações mencionadas situam-se comprovadamente na proximidade imediata de estações terrestres regulares de satélites de comunicações.

A título de ilustração, observa-se a localização de algumas estações do sistema Echelon, distribuidas em solo e no espaço na figura 2 e a imagem ótica de satélite de uma estação na figura 3.

Figura 2 – Estações de monitoração do sistema



Fonte: *Universität Lüneburg, 2005*

[6] INTELSAT (International Telecomunications Satellite Organisation) foi fundada em 1964 como uma autoridade dotada de uma estrutura organizacional, semelhante à das Nações Unidas, com o objetivo comercial de operar as comunicações internacionais.

Figura 3 - Bad Aibling, Alemanha



Fonte: Goolge Earth, 2009

3.3 Evolução do sistema

Após o final da década de 1990, há pouco material publicado sobre o tema em estudo, sendo que os textos disponíveis na internet frequentemente repetem os conteúdos apresentados anteriormente.

Desde meados dos anos 90, as agências de inteligência de comunicações enfrentaram dificuldades substanciais em manter o acesso global aos sistemas de comunicações. Estas dificuldades aumentaram após o ano de 2000, principalmente em virtude do deslocamento das telecomunicações para as redes de fibra ótica de capacidade elevada, pois o acesso físico aos cabos dificulta a interceptação.

Por outro lado, verificou-se que a demanda de comunicações via satélite vêm aumentando ao longo do tempo, principalmente em função de fatores como a evolução da tecnologia de lançamento de satélites, com redução de custos, e aumento da capacidade de transmissão dos que estão sendo lançados no espaço, tornando esses serviços mais acessíveis.

Deduz-se que a tendência futura em SIGINT é a do aumento nos investimentos na coleta espacial de COMINT, do maior uso de fontes humanas para obter códigos criptográficos e da intensificação de esforço para se penetrar em sistemas de informática estrangeiros, usando a Internet e outros meios.

4 Sistemas concorrentes

Conforme já foi tratado, para se realizar interceptações das comunicações

internacionais transmitidas por satélites a nível mundial são indispensáveis estações de recepção no Atlântico, no Oceano Índico e na região do Pacífico.

Teoricamente, França e Rússia possuem territórios sob influência política nas três regiões citadas e poderiam igualmente explorar um sistema de intercepção mundial, considerando os pressupostos ténicos e financeiros para o empreendimento. Contudo, não há um número suficiente de informações disponíveis no domínio público para poder afirmar que esse é o caso.

5 Reflexos para o Brasil

No Brasil, atualmente, observa-se o emprego de uma variada quantidade de meios de comunicações, desde os mais simples até os mais sofisticados que utilizam salto de freqüência e criptografia, microondas, satélites e fibra ótica.

Nos dias atuais, os sistemas de informatizados que trafegam pela internet podem estar vulneráveis, dependendo de suas características.

No Sistema Brasileiro de Inteligência (SISBIN) não houve evolução tecnológica (SIGINT) considerável capaz de fazer frente às novas ameaças.

A vulnerabilidade de ser “alvo” do sistema Echelon é a possibilidade de vazamento de assuntos estratégicos para o país. Exemplo disso é o caso Sistema de Proteção da Amazônia (SIPAM), citado no relatório do Parlamento Europeu (2001) envolvendo interceptação (NSA) da negociação entre a Thomson-CSF e o Brasil e transmissão dos resultados Raytheon Corp.

6 Conclusão

O Echelon se constitui num elevado fator de risco para a soberania de qualquer país, sendo que o verdadeiro perigo é o de não adotar medidas preventivas que possam minimizar as vulnerabilidades dos sistemas de telecomunicações.

Existe a necessidade de técnicos especializados para assessorar o SISBIN no acompanhamento destas questões estratégicas, apoiados pela Agência Nacional de Telecomunicações (ANATEL), com a finalidade de se adotarem medidas preventivas.

Finalmente, a ameaça que o Echelon apresenta para a vida privada e a economia não devem ser vistas apenas em função do poderoso sistema de vigilância eletrônica que representa, mas pelo fato de operar num espaço praticamente à margem da lei.

Referências

Bamford, James, Body of Secrets. Anatomy of the Ultra-Secret National Security Agency. From the Cold War through the Dawn of a new Century, Doubleday Books (2001).

Bamford, James, The Puzzle Palace. *Inside the National Security Agency, America's most secret intelligence organization, Penguin Books* (1983).

Campbell, Duncan, Inside Echelon, Heise Online, 24.7.2000, Disponível em: *www.heise.de/tp/deutsch/special/ech/6928/1.html.* Acesso em: 27 de abr. de 2009.

Campbell, Duncan, Somebody's listening, Tehy've got it taped, 12.8.1988, New Statesman. Disponível em: www.jya.com/Echelon-dc.htm. Acesso em: 2 de jun. 2009.

Costa, Silvio, O Sistema Echelon de espionagem global ou a lei do vale tudo, Revista Espaço Acadêmico – Ano II – Nº 22 – Março de 2003 – Mensal – Disponível em: www.espacoacademico.com.br/022/22ccosta.htm. Acesso em 25 de maio de 2009.

Departament of the Army, Field Manual Nº. 2-0, INTELLIGENCE, Washington, DC: 2010. Disponível em: www.fas.org/irp/doddir/army/fm2-0.pdf. Acesso em 02 de junho de 2010.

Frost, Mike in Fernsehinterview von NBC "60 Minutes" vom 27.2.2000, Disponível em: www.cryptome.org/Echelon-60min.htm. Acesso em 25 de maio de 2009.

Orlovski, Johannes, Echelon: Welche Hinweise gibt es auf die tatsächliche Existenz des vorwiegend amerikanisch-britischen Echelon-Systems und wie funktioniert das System?, Seminarbeit Security-Management, Universität Lüneburg, Deutschland, 2005

Parlamento Europeu, Relatório sobre a existência de um sistema global de interceptação de comunicações privadas e econômicas (sistema de interceptação “Echelon”), elaborado por Comissão Temporária sobre o Sistema de Interceptação Echelon, Portugal: 2001. Disponível em: http://www.fas.org. Acesso em 12 de maio de 2009.

Potengy, Silvio, “Echelon” X SEGURANÇA NACIONAL, Revista da Escola Superior de Guerra nº 39, Brasil, 2000.